PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-102735
(43)Date of publication of application : 16.04.1996

(51)Int.Cl. H04L 9/32
G06F 13/00
G06F 17/21
G09C 1/00

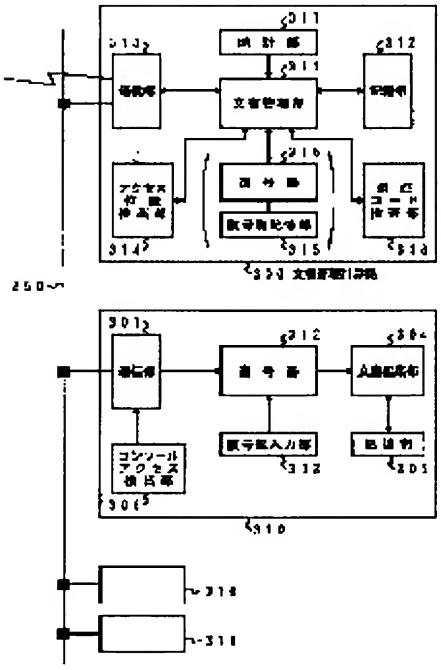
(21)Application number : 06-238143
(22)Date of filing : 30.09.1994

(71)Applicant : TOSHIBA CORP
(72)Inventor : SHINPO ATSUSHI

(54) ELECTRONIC DOCUMENT PROCESSING METHOD

(57)Abstract:
PURPOSE: To improve the delivery flexibility of an electronic document by protecting the contents of the document to the computer manager of a receiver system when the electronic document is delivered to a 2nd computer system that is used by a receiver from a 1st computer system that is used by a transmitter.

CONSTITUTION: The position of an access requester client 310 is detected in a network 350 by an access position detection part 314 of a document management server 300 and a console access detection part 306 of the client 310. A network address is set for an access requester computer 310 to permit an access in regard of the reading issue. Each client 310 is provided with a detection part 306 and therefore able to have a remote access. The part 314 requests such services as the transfer of a file, a virtual terminal, a network file system, etc., and checks not only the address of the requester computer but the name of a requester user and excludes the access that is performed by a log-in operation.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－102735

(43)公開日　平成８年(1996)４月16日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/32					
Ｇ０６Ｆ	13/00	３５１　Ｚ	7368－5E			
	17/21					
				Ｈ０４Ｌ　9/ 00		Ａ
			9288－5L	Ｇ０６Ｆ　15/ 20	５９６　Ｚ	

審査請求　未請求　請求項の数３　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平6－238143

(22)出願日　平成６年(1994)９月30日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

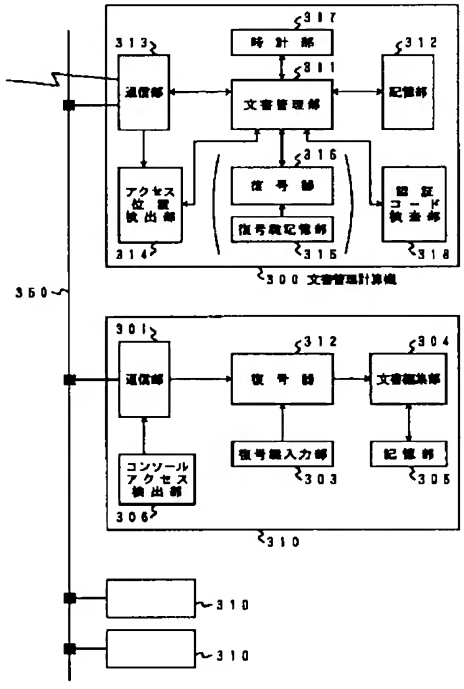
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　電子文書処理方法

(57)【要約】

【目的】　電子文書の送り先計算機にて読出し可能な利用者、その時刻や場所を送信文書ごとに指定できる電子文書処理方法を提供すること。

【構成】　第１の計算機システムから送信された電子文書を第２の計算機システムにて受信し、該第２の計算機システムへの該電子文書に対する読み出し要求に応じた処理を行うための電子文書処理方法において、送信された、所定の暗号鍵で暗号化された電子文書および該電子文書の読み出し条件を示すデータを受信する受信ステップと、外部から前記暗号化された電子文書の読み出し要求を受けた場合、前記読み出し条件に応じて、該要求を許可するか否かを決定する決定ステップと、この決定ステップにて前記要求を許可することが決定された場合、前記所定の暗号鍵に対応する所定の復号鍵を獲得し、該復号鍵で前記暗号化された電子文書を復号する復号ステップとを有することを特徴とする。



1

【特許請求の範囲】

【請求項１】第１の計算機システムから送信された電子文書を第２の計算機システムにて受信し、該第２の計算機システムへの該電子文書に対する読み出し要求に応じた処理を行うための電子文書処理方法において、

送信された、所定の暗号鍵で暗号化された電子文書および該電子文書の読み出し条件を示すデータを受信する受信ステップと、

外部から前記暗号化された電子文書の読み出し要求を受けた場合、前記読み出し条件に応じて、該要求を許可するか否かを決定する決定ステップと、

この決定ステップにて前記要求を許可することが決定された場合、前記所定の暗号鍵に対応する所定の復号鍵を獲得し、該復号鍵で前記暗号化された電子文書を復号する復号ステップとを有することを特徴とする電子文書処理方法。

【請求項２】第１の計算機システムから送信された電子文書を第２の計算機システムにて受信し、該第２の計算機システムへの該電子文書に対する読み出し要求に応じた処理を行うための電子文書処理方法において、

送信された、電子文書および該電子文書の読み出しを許可する日時の情報と読み出しを許可する要求元の存在場所の情報の少なくとも一方を含む読み出し条件を示すデータを受信する受信ステップと、

外部から前記暗号化された電子文書の読み出し要求を受けた場合、前記読み出し条件に時間の情報が含まれるときは現在の時間を獲得するとともに、前記読み出し条件に要求元計算機の存在場所の情報が含まれるときは該読み出し要求を発生した計算機のアドレスからその存在場所を特定する情報を獲得し、獲得した該情報と前記受信ステップにて得られた読み出し条件を示すデータとを対比することにより、前記読み出し要求を許可するか否かを決定する決定ステップとを有することを特徴とする電子文書処理方法。

【請求項３】前記受信ステップでは、前記電子文書および前記読み出し条件を示すデータとともに、該読み出し条件を示すデータが改ざんされたことを検出し得る認証コードを取り込み、

前記決定ステップでは、前記読み出し要求が与えられた場合、最初に前記認証コードを検査し、この検査の結果、前記読み出し条件を示すデータが改ざんされていないことが確認された場合に前記読み出し要求を許可するか否かを決定することを特徴とする請求項１または２に記載の電子文書処理方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、電子文書を事前に通信ネットワーク経由で送り先に配送し、送信者により指定された条件が成立した場合にその内容を公開できるようにした電子文書配送システムに関する。

2

【０００２】

【従来の技術】電子会議システムあるいは計算機会議システムが徐々に普及してはいるものの、実際に人間が移動して行なう対面会議が完全になくなるとは考えにくい。これは、直接対面した場合とほぼ等価な臨場感を計算機会議で実現することは不可能と考えられることが一因である。

【０００３】その一方で、対面会議の場面に計算機技術による支援機能がより入り込むことは予想される。例えば、文書の配布や発言、議論の保存・記録はより電子化されていくだろう。移動先で必要となる文書が予め分かっていればそれを移動先に送りつけておき、実際に移動先に到着後、その文書を利用する形態も必要となるだろう。いわば、電子文書の宅配である。

【０００４】従来、電子文書の配送方法としてはフロッピーディスクなどの２次記憶媒体に記録して配る方法、電子メールなどの計算機間の通信を利用して配る方法が存在する。このうち、通信ネットワークを利用する後者の方法において、通信路上のデータ保護が必要な場合には、通信データの暗号化が行なわれる。具体例としては、Ｉｎｔｅｒｎｅｔなどで実現されている暗号電子メール（ＰｒｉｖａｃｙＥｎｈａｎｃｅｄ　Ｍａｉｌ）がある。但し、従来の暗号電子メールは、基本的には特定計算機の特定ユーザ宛に電子文書を暗号化して配送する機能を実現するだけであり、通信路での盗聴防止や文書の改ざん検出を実現するが、例えば移動先の計算機の管理者（ｒｏｏｔ）には送信された文書は全て内容が読まれる可能性がある。これは、暗号電子メールの復号に必要な秘密鍵は通常、ユーザのホームディレクトリにファイルとして置かれているが、ｕｎｉｘファイルシステムのアクセス制御を利用して他のユーザからの利用を制限しているのみであり、管理者は特権として任意のファイルのアクセス権を変更可能であるためである。

【０００５】また、会議での利用文書を想定すると、会場に到着した会議のメンバに対しては、文書を送信した本人が到着していなくても内容を読まれても構わないとか、あるいは、その会場に行かないメンバに対しては文書の配送を行なわないなどの文書内容の読み出しに対するきめ細かな設定が行なえることが望ましいが、このような機能は、電子文書配送システムでは提供されていなかった。

【０００６】

【発明が解決しようとする課題】このように、暗号電子メールに代表される従来の電子文書配送システムでは、送り先の計算機システムの管理者により送信文書の内容が読まれる可能性があった。また、文書の読み出し条件が固定的であるため、読み出しを許可する日時や場所、ユーザの指定が不可能であったり、柔軟性に欠けるなどの問題点があった。

【０００７】本発明は、上記事情を考慮してなされたも

のであり、電子文書の送り先の計算機において、読み出し可能な利用者およびその時刻や場所を送信文書ごとに指定可能できる電子文書処理方法を提供することを目的とする。

【０００８】また、本発明は、上記事情を考慮してなされたものであり、電子文書の送り先の計算機の管理者に対しても内容の保護を実現できるとともに、読み出し可能な利用者およびその時刻や場所を送信文書ごとに指定できる電子文書処理方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】本発明は、第１の計算機システムから送信された電子文書を第２の計算機システムにて受信し、該第２の計算機システムへの該電子文書に対する読み出し要求に応じた処理を行うための電子文書処理方法において、送信された、所定の暗号鍵で暗号化された電子文書および該電子文書の読み出し条件を示すデータを受信する受信ステップと、外部から前記暗号化された電子文書の読み出し要求を受けた場合、前記読み出し条件に応じて、該要求を許可するか否かを決定する決定ステップと、この決定ステップにて前記要求を許可することが決定された場合、前記所定の暗号鍵に対応する所定の復号鍵を獲得し、該復号鍵で前記暗号化された電子文書を復号する復号ステップとを有することを特徴とする。

【００１０】また、本発明は、第１の計算機システムから送信された電子文書を第２の計算機システムにて受信し、該第２の計算機システムへの該電子文書に対する読み出し要求に応じた処理を行うための電子文書処理方法において、送信された、電子文書および該電子文書の読み出しを許可する日時の情報と読み出しを許可する要求元の存在場所の情報の少なくとも一方を含む読み出し条件を示すデータを受信する受信ステップと、外部から前記暗号化された電子文書の読み出し要求を受けた場合、前記読み出し条件に時間の情報が含まれるときは現在の時間を獲得するとともに、前記読み出し条件に要求元計算機の存在場所の情報が含まれるときは該読み出し要求を発生した計算機のアドレスからその存在場所を特定する情報を獲得し、獲得した該情報と前記受信ステップにて得られた読み出し条件を示すデータとを対比することにより、前記読み出し要求を許可するか否かを決定する決定ステップとを有することを特徴とする。

【００１１】また、好ましくは、前記受信ステップでは、前記電子文書および前記読み出し条件を示すデータとともに、該読み出し条件を示すデータが改ざんされたことを検出し得る認証コードを取り込み、前記決定ステップでは、前記読み出し要求が与えられた場合、最初に前記認証コードを検査し、この検査の結果、前記読み出し条件を示すデータが改ざんされていないことが確認された場合に前記読み出し要求を許可するか否かを決定するように構成すると良い。

【００１２】

【作用】本発明では、送信者が利用する第１の計算機システムから、受信者が利用する第２の計算機システム、例えば会議場に設けられた計算機システムなどに、事前に電子文書を送信し、送信者が第２の計算機システムの設置場所に到着した後で送信しておいた電子文書を読み出して利用する際に、次のような処理が行われる。

【００１３】すなわち、第２の計算機システムでは、第１の計算機システムから送信された、所定の暗号鍵で暗号化された電子文書および該電子文書の読み出し条件を示すデータを受信した後、外部から前記暗号化された電子文書の読み出し要求を受けた場合、前記読み出し条件に応じて、該要求を許可するか否かを決定する。ここで、前記要求を許可することが決定された場合に初めて、前記所定の暗号鍵に対応する所定の復号鍵を獲得し、該復号鍵で前記暗号化された電子文書を復号することができる。

【００１４】このとき、電子文書を復号化するための復号鍵は読み出し時に入力するので、復号鍵の所持者だけが復号処理を可能とすることができ、第２の計算機システムの管理者であっても配送鍵を知らない限りは内容を読むことはできない。例えば、配送鍵を事前に会議のメンバ全員で共有しておけば、会議のメンバは読み出しができる。このように配送鍵の管理により内容の読み出しが可能となる受信者を特定することができる。

【００１５】さらに、第２の計算機システムが、送信文書に添付された読み出し条件に応じてアクセス制御を行なうことができるので、例えばアクセス日時の制限（いつからいつの間であれば取り出しができるなど）やアクセス場所の制限（会場内の計算機からでないと取り出しができないなど）を設定可能で、様々な読み出し条件に応じてきめ細かな制御が行なえる。

【００１６】一方、本発明では、送信者が利用する第１の計算機システムから、受信者が利用する第２の計算機システム、例えば会議場に設けられた計算機システムなどに、事前に電子文書を送信し、送信者が第２の計算機システムの設置場所に到着した後で送信しておいた電子文書を読み出して利用する際に、次のような処理が行われる。

【００１７】すなわち、第２の計算機システムでは、第１の計算機システムから送信された、電子文書および該電子文書の読み出しを許可する日時の情報と読み出しを許可する要求元の存在場所の情報の少なくとも一方を含む読み出し条件を示すデータを受信した後、外部から前記暗号化された電子文書の読み出し要求を受けた場合、現在の時間や該要求の発生元計算機の存在場所を特定する情報を獲得し、獲得した該情報と読み出し条件とを対比して、前記読み出し要求を許可するか否かを決定する。

【００１８】このとき、第２の計算機システムが、送信

文書に添付された読み出し条件に応じてアクセス制御を行なうことができるので、アクセス日時の制限（いつからいつの間であれば取り出しができるなど）やアクセス場所の制限（会場内の計算機からでないと取り出しができないなど）を設定可能で、様々な読み出し条件に応じてきめ細かな制御が行なえる。

【００１９】

【実施例】以下、図面を参照しながら本発明の実施例を説明する。図１は、本発明の一実施例に係る電子文書配送システムの概略的な構成を示す。このシステムは、送信者が通常利用している計算機システム（以下、ホームシステムと呼ぶ）１０１、送信者の電子文書の送り先となる計算機システム（以下、移動先システムと呼ぶ）１０２、通信ネットワーク１０３からなる。

【００２０】移動先システム１０２は、例えば会議などで一時的に使用される計算機環境であっても良い。通信ネットワーク１０３は、例えば広域ネットワークである。この電子文書配送システムは、最低限、１つのホームシステム１０１と１つの移動先システム１０２にて構成されるが、現実的には、ホームシステム１０１を複数備えることが想定され、さらには移動先システム１０２をも複数備えることも考えられる。また、１つの計算機システムに、ホームシステム１０１としての機能と移動先システム１０２としての機能を兼備させることも可能である。

【００２１】本実施例では、ホームシステム１０１は、通信ネットワーク１０３に収容される１つのサブネットを構成しており、例えば、ルータあるいはゲートウェイなどの網間接続装置１２０、後述するような機能を有する少なくとも１台の端末計算機２００、ローカルネットワーク３４０から構成される。

【００２２】また、移動先システム１０２は、通信ネットワーク１０３に収容される１つのサブネットを構成しており、例えば、ルータあるいはゲートウェイなどのような網間接続機能および後述するような文書管理機能を有する文書管理計算機３００、後述するような機能を有する少なくとも１台の端末計算機３１０、ローカルネットワーク３５０から構成される。ただし、文書管理計算機３００の機能のうち網間接続機能を取り出し、ホームシステム１０１のように網間接続装置を設ける構成にしても構わない。

【００２３】なお、ホームシステム１０１は、サブネットを構成せずに、ネットワークに接続できる機能を有する１台の計算機２００とすることも可能であり、移動先システム１０１は、ネットワークに接続できる機能、計算機３００の機能、計算機３１０の機能を兼ね備えた１台の計算機とすることも可能である。

【００２４】また、ホームシステム１０１や移動先システム１０２は、これらの他に、種々の構成が考えられる。前述したように図１のホームシステム１０１と移動先システム１０２は、通信ネットワーク１０３を介して接続されている。ホームシステム１０１と移動先システム１０２はそれぞれ、電子文書を相互に送受信する手段、例えば、電子メールやファイル転送プログラム（ｆｔｐもしくはＡｎｏｎｙｍｏｕｓ　ｆｔｐなど）を備えている。

【００２５】電子文書の配送主体である送信者は、ホームシステム１０１内の計算機２００から移動先システム１０２内の特定の計算機３１０に向けて電子文書を送信する。このとき、配送主体は、移動先システム１０２に既にアカウントを所持している場合には、ｆｔｐなどにより文書の送信を行なうことができる。アカウントを所持していない場合には、移動先システム１０２内の、Ａｎｏｎｙｍｏｕｓ　ｆｔｐの設定がなされている計算機３１０のＩＰアドレスを知るか、移動先システム１０２に文書を送付するための適当なメールアドレスを知るか、あるいは移動先システム１０２の計算機管理者にアカウントの設定を依頼するなど、文書の送信に必要な処理を行なう。

【００２６】ところで、移動先システム１０２の計算機管理者は、当該システム内のファイルおよびディレクトリの使用権を操作可能であり、送信された文書の内容を読み出すことができる。本実施例では、これを防止し、読み出しが可能となる利用者を限定するために、送信文書を適当な暗号鍵（以下、配送鍵と呼ぶ）で暗号化して送信する。この配送鍵の配布を制御することにより、様々な読み出し条件を設定することが可能となる。例えば、送信者自身が決定した配送鍵を秘密にしておけば、送信者自身しか読むことはできない。あるいは、あるグループで共有されている配送鍵を利用すれば、そのグループのメンバは誰でも読むことができる。さらには、グループのメンバのうち任意のｋ人が協力することにより内容を読むことができるようにするなどの設定が可能である。これらの具体例は、以降で説明する。

【００２７】次に、本実施例の電子文書配送システムのより具体的な構成例を、図２および図３に示す。図２は、ホームシステム１０１内の計算機２００の一例であり、図３は、移動先システム１０２内の文書管理計算機（以下、文書管理サーバと呼ぶ）３００とそのクライアントである計算機（以下、クライアントと呼ぶ）３１０の一例である。

【００２８】図２のようにホームシステム１０１内の計算機２００は、電子文書を編集する文書編集部２０１、編集した文書を保存する記憶部２０２、送信文書の暗号化に利用する配布鍵を生成する配布鍵生成部２０３、配布鍵をＩＣカードやフロッピーディスクなどから入力し、また配布鍵生成部２０３により生成された配布鍵をＩＣカードやフロッピーディスクなどへ出力する配布鍵入出力部２０４、配布鍵を利用して電子文書を暗号化する暗号器２０５、暗号器２０５への鍵の入力の切替え、

および生成した配布鍵の出力先の切替えを行なうスイッチ２０６、送り先での読み出し条件を設定する読み出し条件設定部２０７、読み出し条件データに対し認証コードを生成する認証コード生成部２０８、暗号化された文書と認証コード付きの読み出し条件データを所定のフォーマットで合成するフォーマット合成部２０９、以上により作成された文書を送信する通信部２１０を有する。

【００２９】読み出し条件データは、移動先システム１０２において、受信した文書の読み出しを制御する文書管理サーバ３００が、リード要求を受理するか拒絶するかを判定するための基準となるデータである。一例として、移動先システム１０２でのログイン名、読み出し可能な時刻、読み出しを許可するクライアント３１０（どのクライアント３１０からの読み出し要求であれば許可するか）などを指定したデータである。

【００３０】認証コードは、特定の送信者が設定したデータ内容が第三者により変更されていないかどうかを検査するために付与されるものである。一例としては、利用者に固有の秘密鍵を利用したディジタル署名によって行われる。

【００３１】一方、図３のように移動先システム１０２内には、文書管理サーバ３００とそれ以外のクライアント３１０が存在し、ローカルネットワーク３５０で接続されている。

【００３２】クライアント３１０は、移動先システム１０２にてユーザがコンソールとして使用するための計算機であり、通常複数台用意される。ただし、１台でも構わない。

【００３３】ユーザが使用するクライアント３１０は、ローカルネットワーク３５０を介してデータの入出力を行なう通信部３０１、文書管理サーバ３００から受信した暗号化文書の復号を行なう復号器３０２、復号に用いる鍵をＩＣカードやフロッピーディスクなどから入力する復号鍵入力部３０３、文書を編集する編集部３０４、文書を保存する記憶部３０５、利用者がコンソールから利用しているかあるいはリモートからアクセスしているかを検出するコンソール・アクセス検出部３０６を有する。

【００３４】文書管理サーバ３００は、個々の文書に対するアクセス管理を実施する文書管理部３１１、文書を保存する記憶部３１２、外部のシステムやローカルネットワークとの通信を行なう通信部３１３、この通信部３１３へのアクセスデータ（アクセス要求をしたクライアント３１０のアドレス等）を利用して当該文書管理サーバへのアクセス要求をしたクライアント３１０の位置を検査するアクセス位置検出部３１４、時刻情報を出力する時計部３１７、文書に添付された認証コードの正当性の検査を行なう認証コード検査部３１８を有する。なお、さらに当該文書管理サーバに固有の復号鍵を記憶する復号鍵記憶部３１５、この復号鍵を利用して暗号化文書の復号を行なう復号器３１６を備えれば、後述するような機能を得ることができる。

【００３５】アクセス位置検出部３１４、復号器３１６、認証コード検査部３１８は、文書管理部３１１の制御下にある。アクセス位置検出部３１４と時計部３１７の働きにより文書管理部３１１は、アクセス要求をしたクライアント（アクセス元計算機）３１０のローカルネットワーク３５０上の位置に依存したアクセス制御と時刻に依存したアクセス制御を行なうことができる。時計部３１７およびアクセス位置検出部３１４に必要な設定を行なうコマンドは、当該文書管理サーバ３００の管理者にしか行なうことができないように設定しておく。例えばＯＳにＵｎｉｘを用る場合、コマンドの実行ファイルの所有者をｒｏｏｔにし、パーミッションとして所有者（すなわちｒｏｏｔ）に実行権を与える他は、グループおよびその他のユーザには、読み出し、書き込み、実行の権利を与えないようにする。

【００３６】次に、文書管理サーバ３００内のアクセス位置検出部３１４と、クライアント３１０内のコンソール・アクセス検出部３０６により、アクセス要求元のクライアント３１０のネットワーク３５０上の位置を検出する動作を説明する。読み出し条件として、アクセスを許可するアクセス元計算機３１０のネットワークアドレスが設定されているものとする。例えば、移動先システム１０２内の文書管理サーバ３００と同じサブネットに属しているクライアント３１０からのアクセスは受理するが、それ以外からのアクセスは受理しないなどが設定されている。

【００３７】このとき、単にアクセス元計算機のネットワークアドレスを検査するだけでは、不十分な場合がある。例えば、クライアント３１０に遠隔の計算機からリモートログインし、そこから文書管理サーバ３００に読み出し要求を出す場合、文書管理サーバ３００は読み出しを許可すると、その文書はリモートログイン端末であるクライアント３１０を経由して遠隔の計算機で取得されてしまう。このようなことが生じないように本実施例では、各クライアント３１０にコンソール・アクセス検出部３０６を設けてある。例えば、ｕｎｉｘのコマンドｆｉｎｇｅｒで表示される端末名によりコンソール・アクセスを検出できる。例えばアクセス元計算機の端末名がｃｏｎｓｏｌｅあるいはその省略形のｃｏであれば、コンソールからのアクセスであることが分かる。それ以外の場合には、リモートアクセスの可能性がある。

【００３８】文書管理サーバ３００のアクセス位置検出部３１４では、ファイル転送（ｆｔｐ）や仮想端末（ｔｅｌｎｅｔ）、ネットワークファイルシステム（ｎｆｓ）などのサービスを提供するサーバがネットワークからのサービス要求に対して、要求元の計算機のアドレスを検査するだけでなく、要求元計算機に対して例えばｆｉｎｇｅｒコマンドによりコンソールアクセスのユーザ

名を問い合わせ、要求を発したユーザ名と一致しているかどうかを検査する。このようにすれば、リモートログインによりアクセスしている場合を検出し、排除できる。

【００３９】なお、各文書管理サーバ３００ごとにアクセス位置検出部３１４を実装するのではなく、例えば、ネットワーク中に存在する各種サーバ（例えばファイル転送機能を提供するｆｔｐｄサーバ、リモートログイン機能を提供するｔｅｌｎｅｔｄサーバ、透過性のあるファイルシステムを提供するｎｆｓｄサーバなど）をネットワークからの要求に応じて起動するｉｎｅｔｄサーバのみにアクセス位置検出部３１４を実装し、ｉｎｅｔｄでの検査に通った場合に要求したサーバが起動されるようにすると手間が省けて効果的である。

【００４０】次に、図４および図５のフローチャートを参照しながら、本実施例における情報配送手順（図４）および情報取得手順（図５）の一例を説明する。まず、送信者は移動先システム１０２に対する文書配送に必要な情報（移動先システム１０２内の文書管理サーバ３００のＩＰアドレスやアカウント、メールアドレスなど）を取得済みかどうかを判断する（ステップＳ１１）。

【００４１】取得していない場合には、移動先システム１０２の計算機管理者に対し、文書配送に必要な設定を依頼する（ステップＳ１２）。この後、移動先システム１０２の計算機管理者から、送信に必要な情報を受け取る（ステップＳ１３）。この手続きは、既に移動先システム１０２内の文書管理サーバ３００にアカウントを持っている場合などには不要である。

【００４２】次に、電子文書に対して配送鍵を決定し（ステップＳ１４）、電子文書を配送鍵で暗号化する（ステップＳ１５）。さらに、配送文書の読み出し条件を設定する（ステップＳ１６）。読み出し条件データには、認証コードが添付される。さらに、先の暗号化文書と読み出し条件データ、認証コードを所定のフォーマットとしてまとめた文書を移動先１０２に送信する（ステップＳ１７）。

【００４３】一方、送信文書の取り出しは、まず移動先システム１０２のクライアント３１０にログインし（ステップＳ２１）、そのクライアント３１０から文書管理サーバ３００の所定のディレクトリもしくはメールボックスにアクセスして、所望の文書の読み出しを要求する（ステップＳ２２）。文書管理サーバ３００では、個々の文書に設定された読み出し条件と要求元の条件が合致しているか否かを判定する（ステップＳ２３）。

【００４４】条件が合致していれば、通信部３１３を介しての同文書のコピーを許可する。要求元クライアント３１０には、読み出し文書のコピーが送られる（ステップＳ２４）。読み出しに成功した場合には、クライアント３１０に適切な配送鍵を入力し（ステップＳ２５）、暗号を復号することにより内容を読み（ステップＳ２６）、平文として保存したり編集を行なったりすることが可能となる。

【００４５】本実施例では、移動先システム１０２の計算機管理者であっても配送鍵は分からないため、暗号化文書を復号することはできない。次に、本実施例の電子文書配送システムを対面会議に利用し文書の事前配送を行う場合を例として、その具体的な配送方法を説明する。

【００４６】電子文書の配送主体である送信者は、ホームシステム１０１内の計算機（以下、ユーザ計算機と呼ぶ）２００から、移動先システム１０２内のクライアント（以下、会場計算機と呼ぶ）３１０に向けて電子文書を送る。会場計算機３１０に電子文書を送る方法として、一例として電子メールを利用する場合を説明する。

【００４７】会場計算機３１０の管理者は、設定された会議ごとに異なるアカウントを設定する。例えば、ｍｅｅｔｉｎｇ１，ｍｅｅｔｉｎｇ２，…等である。会議の議長は、会議室の予約を会場計算機の管理者に対して要求する。この要求に対し、管理者は予約可能の場合には会場計算機３１０のメールアドレスを返答する。議長は、会議メンバに対して会場計算機３１０のメールアドレスを連絡する。この連絡手段は郵便、電話、電子メールなどのどんな手段によってもよい。このようにして会議のメンバは、会場計算機３１０に電子メールを送信できる状態になる。

【００４８】送信されたメールの読み出しには、ｍｅｅｔｉｎｇ１，ｍｅｅｔｉｎｇ２，…なるアカウントのパスワードが必要であるが、これは会場に到着しないと送信文書を取り出せないようにする場合には会場にて通知することが好ましく、会場以外からリモートログインにより取り出すことを許す場合にはメールアドレスと共に通知しても良い。ただし、ｍｅｅｔｉｎｇ１などのアカウントは、不特定のユーザに解放するものになるので、システムへの攻撃を防ぐ目的から、会議の終了後すみやかに消去するのが良い。パスワードを知る事により、利用者は送られた電子文書の読み出しが可能となる。

【００４９】第１の応用例としては、ユーザ計算機２００上で作成された文書を遠隔地にある会議に持ち込む場合に、事前に会場計算機３１０に送信し、送信者自身が会場に到着した後に、送りつけた文書を取得するシステムである。この場合、電子文書を配送鍵で暗号化して送信するが、配送鍵は送信者が自ら設定し、会議にはその配送鍵を持参する。このようにすると、配送鍵を知らない会議メンバは先に会場に到着し、会場計算機３１０にログインしても暗号化された文書を取得することはできるが、内容を読むことはできない。送信者が到着後、配送鍵を会場にてメンバに配布することにより、他のメンバも内容を読むことができるようになる。このように、電子文書は当日持参せずに、配送鍵を持参するだけで、会議にて資料を配布するのと同様の機能を実現できる。

【００５０】なお、会場にて配送鍵を配布する場合には、各メンバは直接対面しているため、暗号技術による認証方式を利用する必要はなく、暗号鍵を例えば磁気ディスクやＩＣカードに格納して配ったり、あるいは会場のローカルネットワークを介した通信により行なえばよい。

【００５１】第２の応用例は、会議メンバは会場到着時点で事前に配送された文書を自由に読むことのできるシステムである。まず、議長は会場を予約し、会場計算機３１０のメールアドレスを入手する。さらに、議長は乱数により配送鍵を定め、会場計算機３１０のメールアドレスと配送鍵の両方を会議のメンバに配布する。各メンバは会議用文書を配送鍵にて暗号化し、会場計算機３１０のメールアドレスに宛てに送信する。この場合、ｒｌｏｇｉｎやｔｅｌｎｅｔにより会場計算機３１０にメンバのホームシステム１０１内のユーザ計算機２００からログインできれば送られていた暗号化文書を取り出し、配送鍵で復号して内容を読むことができる。実際にメンバが会場にいなければならないようにするためには、最も簡単には会場計算機３１０のアカウント（例えばｍｅｅｔｉｎｇ１）のパスワードを会場で配布するようにする。また、文書管理サーバ３００のアクセス位置検出部３１４の機能を利用することもできる。すなわち、読み出し条件として会場計算機３１０からのアクセスに限定して文書を送信することにより、会場計算機３１０においてリモートログインとログインを識別して、送信文書の取り出しを制限する。

【００５２】実際の会議では、当日になって代理人が出席することが起こり得る。このような場合でも、本発明による方式では、配送鍵と会場計算機３１０のアカウント（および会場計算機３１０のパスワードが事前に配布されている場合にはそのパスワード）を代理人に渡すだけで、代理人が会場に出向けば暗号化文書を読み出すことができる。

【００５３】第３の応用例は、会議メンバのうち何人かが集まると文書を読めるようにする方法である。具体的には、会議メンバｎ人のうち任意のｋ人が会場に到着し、そのｋ人の協力により文書を復号できるような方法である。これは、ｋ－ｏｕｔ－ｏｆ－ｎしきい値法により秘密鍵を分散配布することにより実現できる。すなわち、次の手順による。

【００５４】準備として、各メンバには公開の暗号化鍵と秘密の復号鍵が割り当てられているものとする。この暗号化鍵と復号鍵は公開鍵暗号の鍵である。電子文書の送信者は配布鍵を生成し、文書を配布鍵で暗号化する。さらに、配布鍵をｋ－ｏｕｔ－ｏｆ－ｎしきい値法によりｎ個のピースに分割する。このピースは任意のｋ個を集めると元の配布鍵が復元できる。このｋ－ｏｕｔ－ｏｆ－ｎしきい値法は、例えば文献「暗号とデータセキュリティ」、Ｄ．Ｅ．Ｒ．デニング著、上園・小嶋・奥島訳、培風館、ｐｐ．１８６－ｐｐ．１９２にて詳しく述べられている。これらのピースの１つ１つをそれぞれのメンバの公開暗号化鍵で暗号化したｎ個の暗号化ピースを、暗号化文書に連結して会場計算機３１０に送る。会場にｋ人が到着したら、そのｋ人はめいめいが１つずつ暗号化ピースを平文のピースにする。このｋ個の平文ピースから配布鍵を復元し、配布鍵を利用して暗号化文書の内容を読むことができる。

【００５５】第４の応用例は、指定された時刻のみ配送文書の取り出しを許可するシステムである。この場合、会場の文書管理サーバ３００には、復号器３１６、および固有の公開鍵暗号の暗号化鍵（公開）と復号鍵（秘密）を格納した復号３１５を設ける。送信者は、電子文書を会議メンバに予め配られた配送鍵と会場の文書管理サーバ３００の暗号化鍵で２重に暗号化して送信する。さらに、読み出し条件として文書の復号を許可する日時の範囲を指定する。読み出し条件データには認証コードが付けられる。会場計算機３１０は、送信文書の取り出しが依頼されると、まず読み出し条件データの認証コードを検査する。正当性が確認された場合には、その内部の時計部３１７を参照し、読み出し許可範囲の日時の場合には、文書管理サーバ３００に固有の復号鍵を利用して文書を復号して出力する。会場の文書管理サーバ３００により復号された文書は、会議のメンバがさらに配送鍵で復号することにより内容を読むことができる。この応用例にて、会場計算機３１０の暗号化鍵だけで暗号化して配送することによっても、指定の時刻による取り出しを制限することができるが、例えば指定時刻での別の会議のメンバにより復号される可能性があり、これを防ぐためには、上記のように特定の会議メンバ用の配送鍵で２重に暗号化する方が好ましい。

【００５６】また、他の応用例として、会場計算機３１０にてすべき復号処理を文書管理サーバ３００に行わせるように構成し、文書管理サーバ３００から会場計算機３１０には、平文を与えるようにすることも可能である。また、本発明は上述した各実施例に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【００５７】

【発明の効果】以上説明したように、本発明によれば、送信者が利用する第１の計算機システムから、受信者が利用する第２の計算機システムに電子文書を配送する場合に、送り先システムの計算機管理者に対して内容を保護可能となる。

【００５８】さらに、送信者自身が受信して利用したり、グループの任意のメンバが利用したりするなど、利用者を柔軟に設定できる。また、読み出しの日時や場所を特定するなどの設定も可能であり、送信文書の読み出し条件を様々に設定可能な柔軟な電子文書の配送システムが構築できる。

【図面の簡単な説明】

【図１】本発明の一実施例に係る電子文書配送システムの概略構成を示す図

【図２】ホームシステムの内部構成の一例を示す図

【図３】移動先システムの内部構成の一例を示す図

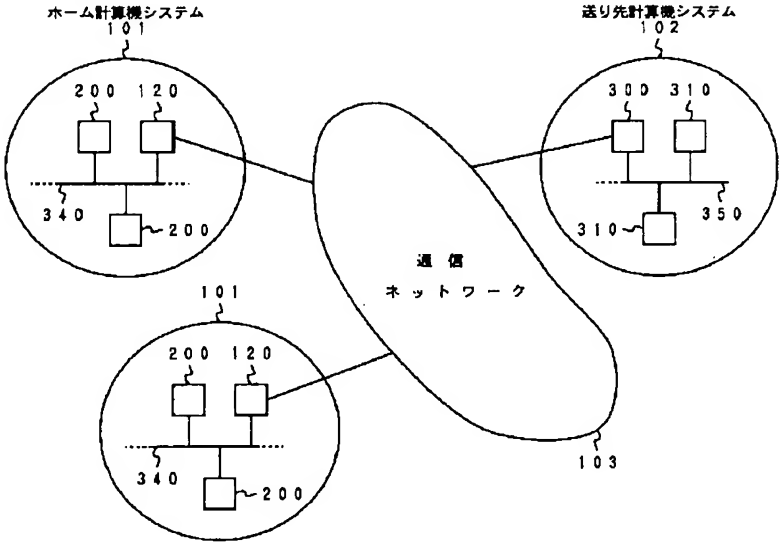
【図４】電子文書配送手順の一例を示すフローチャート

【図５】電子文書取得手順の一例を示すフローチャート

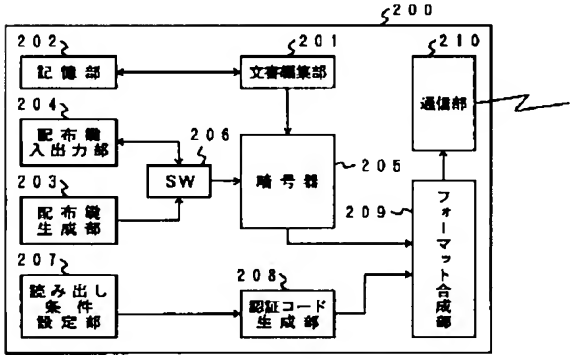
【符号の説明】

１０１…ホーム計算機システム、１０２…送り先計算機システム、１０３…通信ネットワーク、１２０…網間接続装置、２００…ホーム計算機、２０１…文書編集部、２０２…記憶部、２０３…配布鍵生成部、２０４…配布＊鍵入出力部、２０５…暗号器、２０６…スイッチ、２０７…読み出し条件設定部、２０８…認証コード生成部、２０９…フォーマット合成部、２１０…通信部、３００…クライアント計算機、３０１…通信部、３０２…復号器、３０３…復号鍵入力部、３０４…編集部、３０５…記憶部、３０６…コンソール・アクセス検出部、３１０…文書管理計算機、３１１…文書管理部、３１２…記憶部、３１３…通信部、３１４…アクセス位置検出部、３１７…時計部、３１８…認証コード検査部、３１５…復号鍵記憶部、３１６…復号器、３４０，３５０…ローカルネットワーク

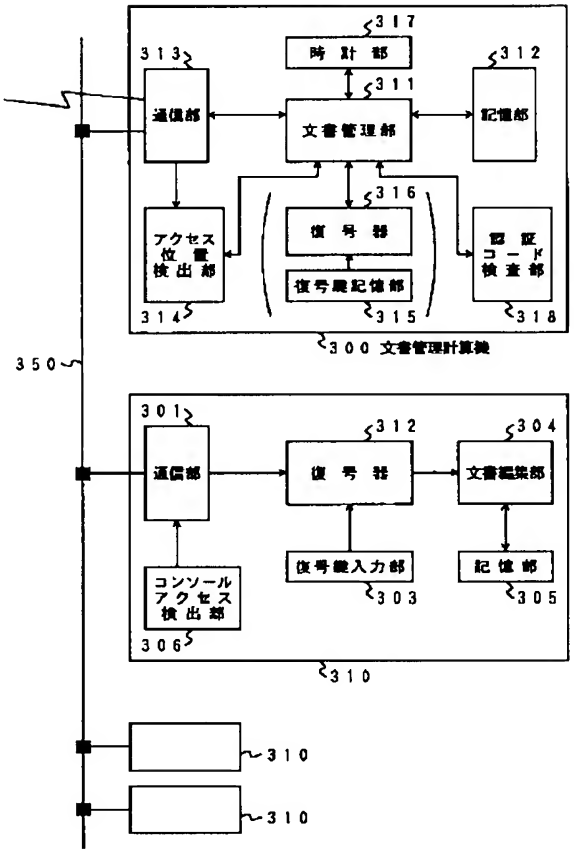
【図１】



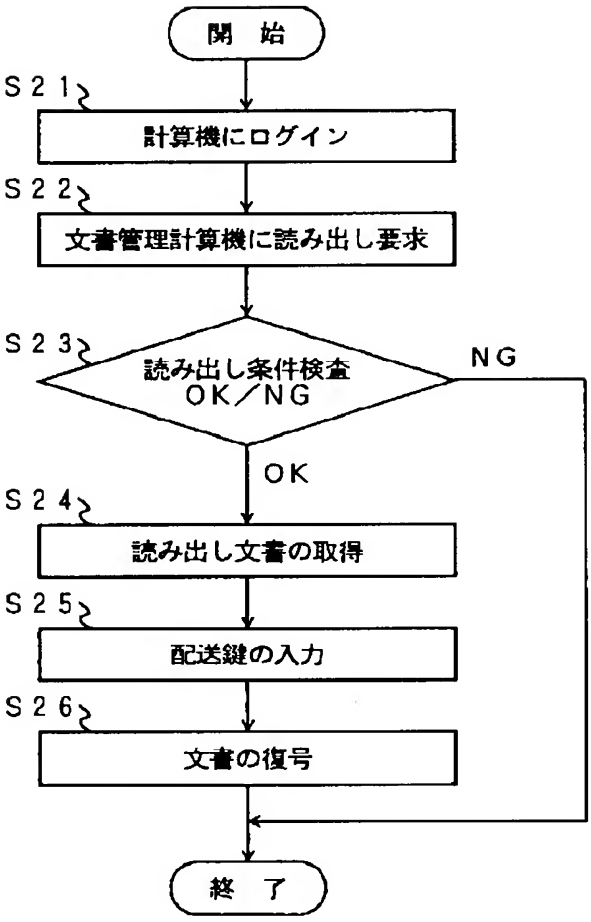
【図２】



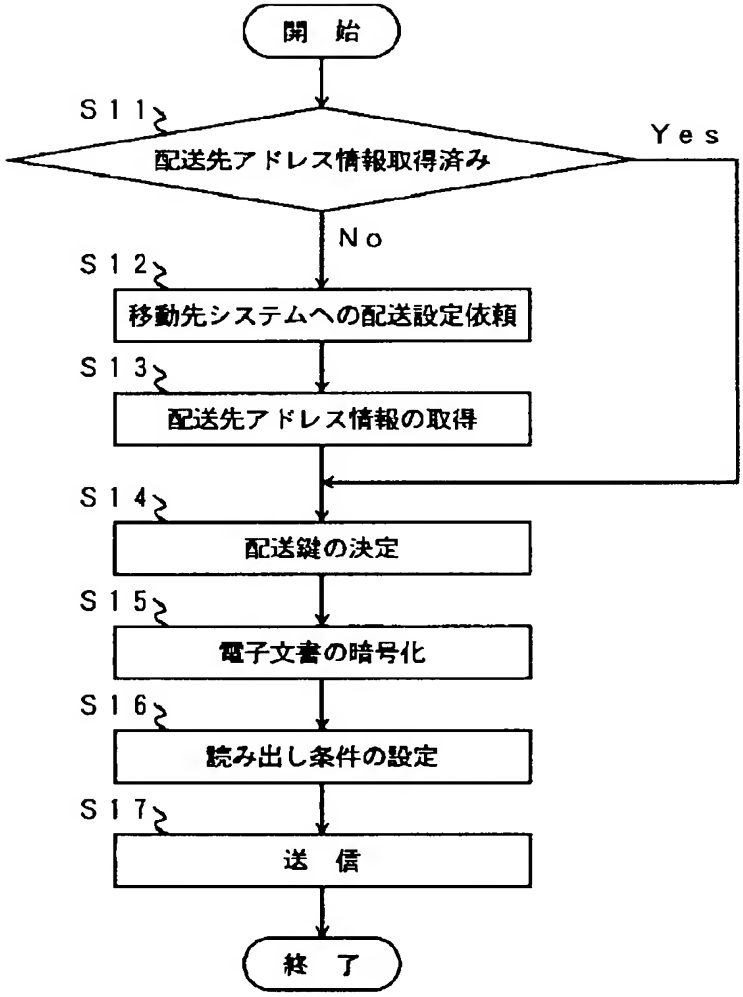
【図３】


317
時計部
313
通信部
311
文書管理部
312
記憶部
316
復号部
アクセス位置検出部
認証コード検査部
復号鍵記憶部
314
315
318
300 文書管理計算機
350
301
通信部
312
復号部
304
文書編集部
コンソールアクセス検出部
復号鍵入力部
記憶部
306
303
305
310
310
310

【図５】


開始
S21
計算機にログイン
S22
文書管理計算機に読み出し要求
S23
読み出し条件検査
OK／NG
NG
OK
S24
読み出し文書の取得
S25
配送鍵の入力
S26
文書の復号
終了

【図４】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０９Ｃ　1/00		7259－5Ｊ		